Safety and Certification Approaches for Ethernet based Aviation Databuses

Yang-Hang Lee, Arizona State University

Philip A. Scandura, Jr., and Elliott Rachlin , Honeywell

FAA Software Conference – July 2005

Project Information

❑ FAA-Sponsored Research

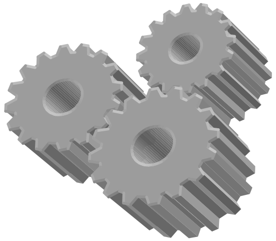
- Project# FAA SDSS BAA – TCBAA-01-0001 “Safety and Certification Approaches for Ethernet-based Aviation Databuses”
- Joint effort between Arizona State University and Honeywell
- Started Oct. 2001 and completed in Dec. 2004.
- Operates under the auspices of the FAA Software and Digital Systems Safety (SDSS) office
- Oversight provided by Charles Kilgore, FAA Program Manager AAR-421, Flight Safety Research (Atlantic City, NJ)

Agenda

- **Ethernet Aviation Databus Project Overview**
- **FAA Databus Evaluation Criteria**
  - CAST-16 Position Paper Overview
  - Applying Generic Criteria
  - Applying Project-Specific Criteria
- **Handbook for *Ethernet-based Aviation Databuses: Certification and Design Considerations***
- **Summary and Conclusions**
- **Contact Information**

Ethernet Aviation Databus Project Overview

Project Summary



This research aims to find ways to make Ethernet acceptable as an aircraft databus !

- ❑ **Objective**
  - ❖ Comprehensive investigation of safety and certification issues of Ethernet based aviation databuses
- ❑ **Goals**
  - ❖ understand any potential safety issues
  - ❖ provide guidance for network structure and operations
- ❑ **Approaches**
  - ❖ examine operations at various software layers and Ethernet network components
  - ❖ workload generation and test strategy
  - ❖ acceptance criteria

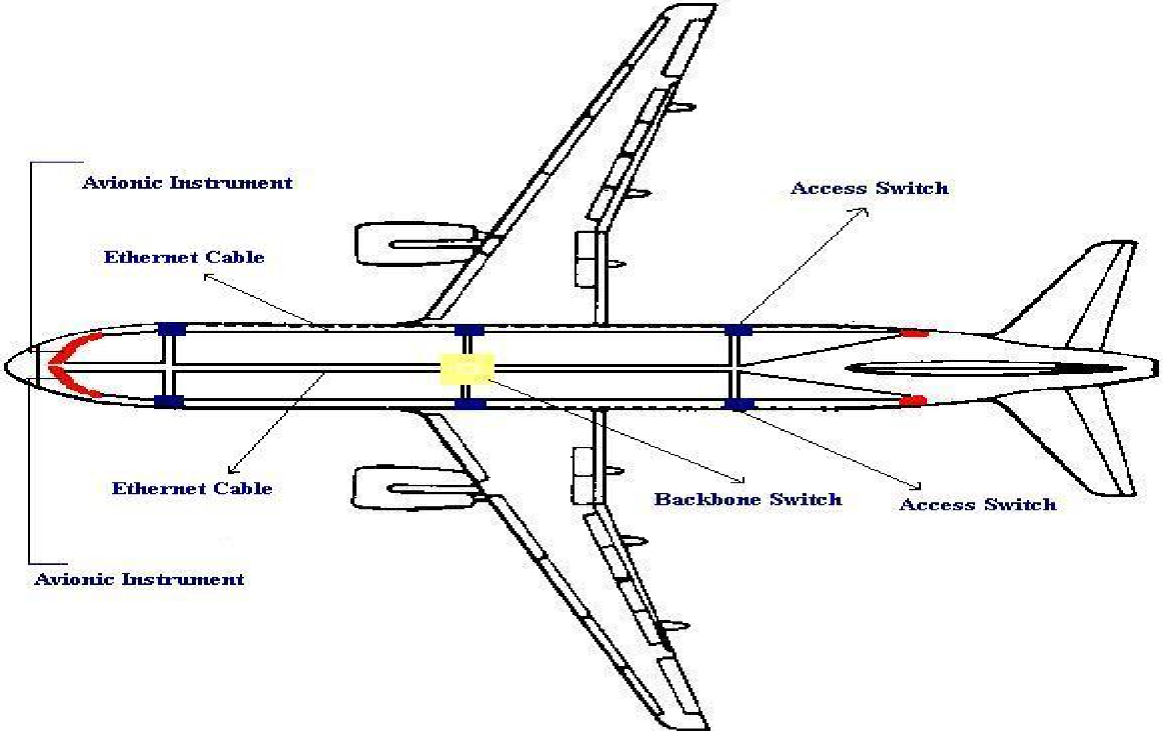
Avionics Databus Technology

- **ETHERNET for aircraft databus !?**
  - Pros: Bandwidth, Full-Duplex, Flexibility – lowers wire counts, and Economical - COTS !
  - Cons: Non-deterministic, and Sensitive to Electro-Magnetic Interference at High speeds (100Mbps)

- **Ethernet must be made suitable for deterministic data transfer before it can be considered as an aviation databus !**
  - Guaranteed delivery
  - Bounded Delays
  - Reliability and fault Tolerance

Ethernet Aviation Databus - Schematic

This is how avionic instruments in a next generation aircraft could be wired !

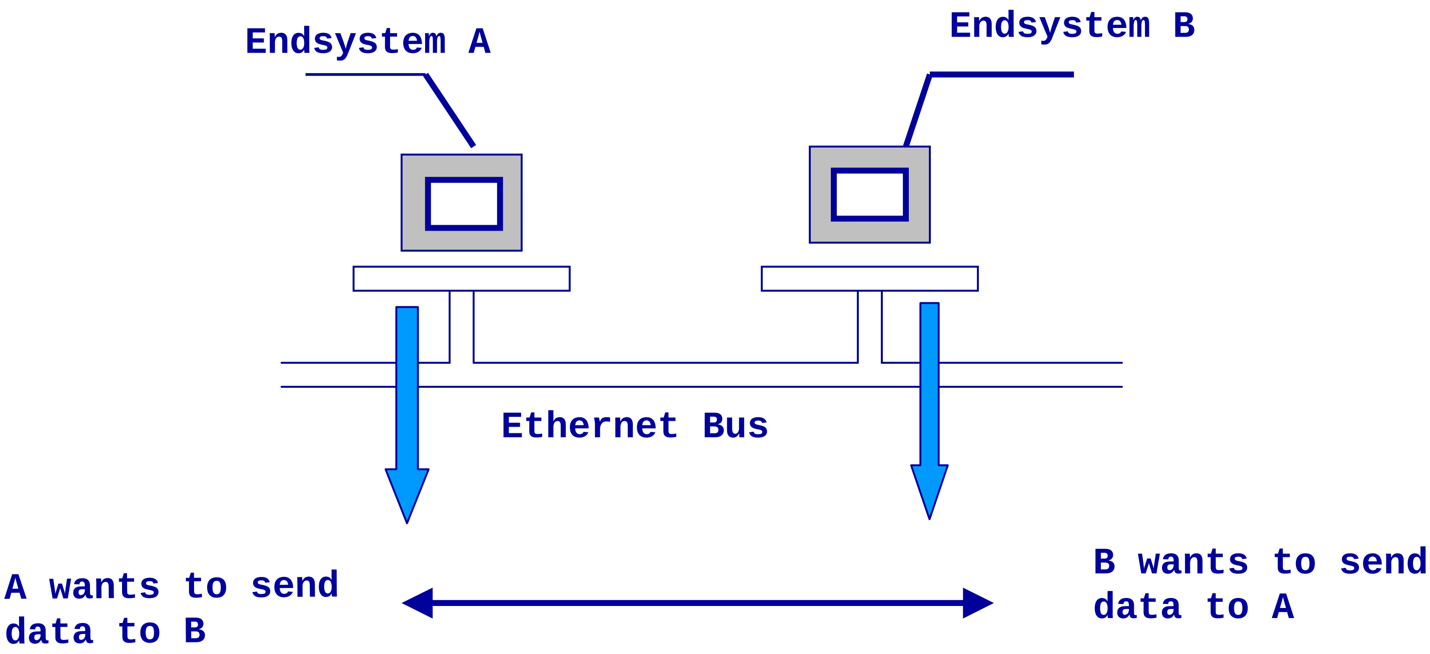


A schematic of the Airbus A320

In Airbus 380 and Boeing 787, Ethernet will be used not only for non-critical operations such as entertainment but also for critical systems such as the flight control systems.

Ethernet System and CSMA/CD

- The standard bus based configuration of Ethernet

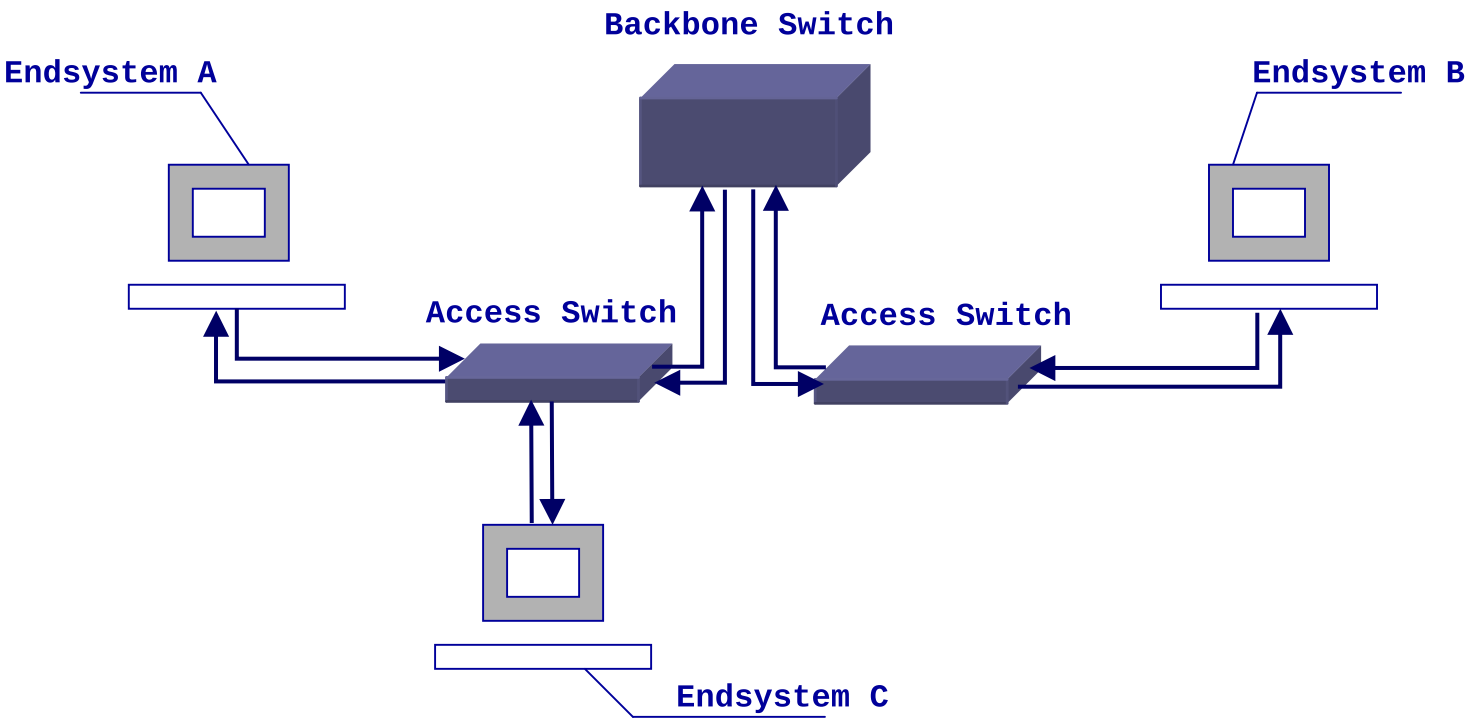


Both A and B sense the carrier (Ethernet bus) to see if it is idle and is ready for data transmission, else if they detect a collision then both back off for a random amount of time before retrying (CSMA/CD)

Switched Ethernet

❑ Switched Ethernet configuration

- no collision on Ethernet bus
- switch: routing at level -2 or –3 and packet buffer



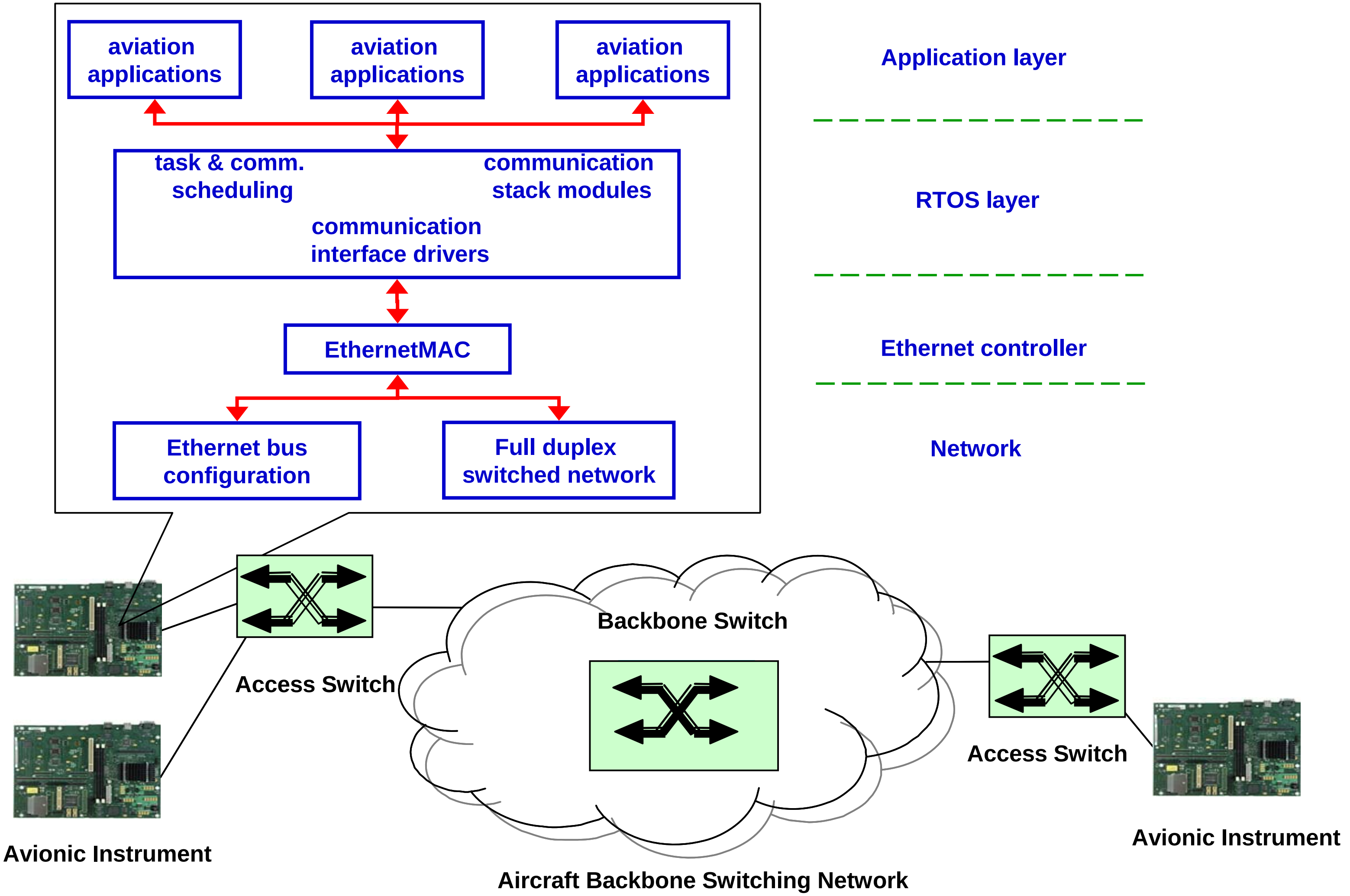
Full Duplex Fully Switched Ethernet

- **Every end-system is connected to a switch, and separate conductors for transmission and reception.**
- **Switches are connected to each other through a backbone switch**
- **There can be no collisions in the system and hence CSMA/CD is turned off. However, non-determinism due to traffic characteristics and system design**
  - Bursty traffic leads to congestion, packet loss and unbounded delays
  - Improper end-system and switch communication architecture can lead to buffer overflows which in turn leads to packet loss
  - Lack of specific policies for real-time traffic can lead to degraded service for high priority data leading to missed deadlines
- **Non-determinism due to the above factors can be overcome**
  - a proper design of the network communication components
  - an analysis of the traffic loads in the system.

Determinism in Ethernet Databus

- **Traffic characteristics**
  - bursty (worst case) and average traffic (data rate, packet size, unicast or multicast)
  - source and destination applications
- **Quality of service requirements**
  - delay and jitter
  - packet loss and system failure rates
- **System architecture**
  - network configuration
  - traffic management, routing, and packet scheduling
- **Analysis and verification**
  - model and analysis
  - testing

Ethernet Aviation Databus – Communication Architecture



aviation applications

aviation applications

aviation applications

task & comm. scheduling

communication stack modules

communication interface drivers

EthernetMAC

Ethernet bus configuration

Full duplex switched network

Application layer

RTOS layer

Ethernet controller

Network

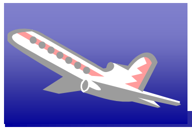
Solutions for Deterministic Operations

Node level

- bound the latencies experienced by a data packet at the end nodes
- regulate transmission traffic (bounded to a pre-defined bursty model)
- schedulable and deterministic communication operations
- handle network failure, packet loss, and bit error

Switch and network level

- Network configuration initialization and static routing → traffic model at each switch element
- Packet scheduling algorithm, analysis of delay and buffer requirement for each switch
- Multicast support, traffic
- Replication (network and packet) for fault tolerance



ARINC 664 - ADN

- **The ARINC 664 specification Aircraft Data Network (ADN)**
  - a multi-part ARINC Standard defining data networking standards recommended for use in commercial aircraft installations.
  - provides a means to adapt commercially defined networking standards to an aircraft environment
  - refers extensively to data networking standards developed by the Internet community and the Institute of Electrical Engineers (IEEE). It also recognizes the ISO specified Open Systems Interconnect (OSI) standards.
- **Part 7 gives a sample implementation of a “Deterministic Network”. We will briefly discuss the salient features of this implementation.**

ADN – Deterministic Network

- **Also called AFDX – Avionics Full Duplex Switched Ethernet. It uses the TCP/IP protocol suite with UDP on top standard IP for data exchange.**

- **Determinism is defined using the following parameters:**
  - Guaranteed bandwidth
  - Maximum latency for data delivery
  - Maximum delay jitter
  - Defined probability of frame loss
  - Maintenance of ordinal integrity
  - Impersonation protection

ADN – Deterministic Network

- **Uses the concept of a “virtual link” (VL) to define the determinism. The parameters discussed previously are defined per-VL.**
- **Some of the mechanisms used to achieve this determinism are:**
  - Traffic shaping at end systems and traffic policing at switches
  - Bandwidth allocation per VL
  - Defined packet processing latency at the switch and end-systems (e.g.: the stack processing latency on end-systems is bounded and lower than the 150us + frame delay)
  - Zero frame loss due to collisions and contention
  - Packet sequencing for each VL
  - Network redundancy

FAA Databus Evaluation Criteria

Databus Evaluation Criteria - Overview

- **Certification Authorities Software Team (CAST)**
- **Position Paper CAST-16, “Databus Evaluation Criteria”**
  - Abstract - A number of new and existing databuses are being proposed for use by aircraft manufacturers. This paper documents criteria that should be considered by databus manufacturers, aircraft applicants, and certification authorities when developing, selecting, integrating, or approving a databus technology in the context of an aircraft project.
- **Available on Aircraft Certification Service Software Website:**
  - http://av-info.faa.gov/software/
  - Released February 2003

> ***CAST PAPER DISCLAIMER:*** *“This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects. It does not constitute official policy or guidance from any of the authorities.”*

Databus Evaluation Criteria - Overview

- **Several areas to consider when evaluating a specific databus technology. CAST-16 identified eight major categories**
  - 3.1 Safety - 9 criteria
  - 3.2 Data Integrity - 12 criteria
  - 3.3 Performance - 10 criteria
  - 3.4 Design/Development Assurance - 2 criteria
  - 3.5 Electromagnetic Compatibility - 4 criteria
  - 3.6 Verification and Validation - 9 criteria
  - 3.7 System Configuration Management - 5 criteria
  - 3.8 Continued Airworthiness - 1 criteria
- **Some categories and evaluation criteria overlap**

Remember that a databus cannot be certified alone - it must be certified as part of a aircraft system or function.

Databus Evaluation Criteria - Overview

- **Much of today's "modern" databus technology is based upon commercial COTS products. This presents several issues that must be addressed**
  - Product licensing, royalties and data rights
  - Availability of databus artifacts in support of design assurance (hardware and software)
  - Suitability of databus hardware and software for avionics environment
  - Obsolescence support and continued airworthiness
  - Databus security
  - Others?
- **Keep these issues in mind as we discuss the eight categories identified by CAST-16**

Addressing these issues requires coordination and cooperation between Databus Supplier, System Integrator, Aircraft Applicant and FAA.

Evaluation of Generic Criteria

- **Regardless of the specific databus technology, the following “generic” categories must be evaluated**

- **3.1 Safety - criteria 1 & 2**
  - Aircraft and system-level safety assessments must include the databus as part of the analysis
  - System-level safety assessment must address databus architecture, implementation, failure detection and reporting features
- **3.4 Design/Development Assurance - all criteria**
  - Databus hardware is assessed to the appropriate design assurance level (per the safety assessment) - e.g., DO-254/ED-80
  - Databus software is assessed to the appropriate design assurance level (per the safety assessment) - e.g., DO-178B/ED-12B

Evaluation of Generic Criteria

- **3.5 Electromagnetic Compatibility - all criteria**
  - More than just satisfying satisfy DO-160D/ED14-D
  - Databus equipment and installation must also consider
    - Emissions dependent upon pulse rise-times, bus speed, topology
    - Differential-mode signaling and transformer-coupled connections
    - RF emissions and susceptibility
    - Effects due to lightning and HIRF
- **3.6 Verification and Validation - all criteria**
  - Evaluation to appropriate standards, e.g.,
    - Environment per DO-160D/ED14-D
    - Hardware per DO-254/ED-80
    - Software per DO-178B/ED-12B
  - Bus verification and validation as an integrated system, including
    - Failure management and recovery scenarios
    - Built-In Test capabilities
    - Performance under degraded modes of operation

Evaluation of Generic Criteria

- **3.7 System Configuration Management - all criteria**
  - Databus configuration control at the aircraft installation level, both from fleet and individual aircraft perspectives
  - Databus configuration control in all phases, from design through production and maintenance
  - Configuration of databus documentation, including industry standards, interface control documents, designer’s guide, installation guide, etc.
- **3.8 Continued Airworthiness - all criteria**
  - Databus performance over the lifetime of the aircraft must be considered including
    - Physical degradation of components and wiring
    - Issues due to in-service modifications and repairs
    - Dealing with obsolesce and system upgrades
    - Providing change impact analysis to determine aircraft impacts

Evaluation of Project-Specific Criteria

- **Definition of an Ethernet Aviation Databus**

  "…a Standard Ethernet (IEEE 802.3) based network with a set of solutions in software and hardware across the network to ensure deterministic data delivery between nodes residing on the network."

- **High Level Requirements Abstraction**
  - Determinism, Fault Tolerance, Data Integrity, Performance, System Interoperability, Scalability, Security

- **The following "project-specific" categories will be assessed as part of the Ethernet Aviation Databus Project**
  - 3.1 Safety - criteria 3..9
  - 3.2 Data Integrity - all criteria
  - 3.3 Performance - all criteria

Evaluation of Project-Specific Criteria

- **Step 1: Define the application level requirement and traffic characteristics**
  - To obtain timing and reliability requirements at component level
  - Traffic characteristics
    - source, destination, packet arrival process, volume
    - network configuration and routing
  - Timing requirement
    - deadline
    - jitter
  - Reliability and safety requirement
    - reliability and availability
    - recovery mechanism
    - redundence management

Evaluation of Project-Specific Criteria

- **Step 2: Demonstrate how deterministic operations are achievable, including the set of issues that need to be addressed in any deterministic communication system,**
  - Network topology
  - Traffic regulation
  - Resource and bandwidth allocation
  - Traffic scheduling
  - Network stack processing
  - Redundancy
  - Network component design

Evaluation of Project-Specific Criteria

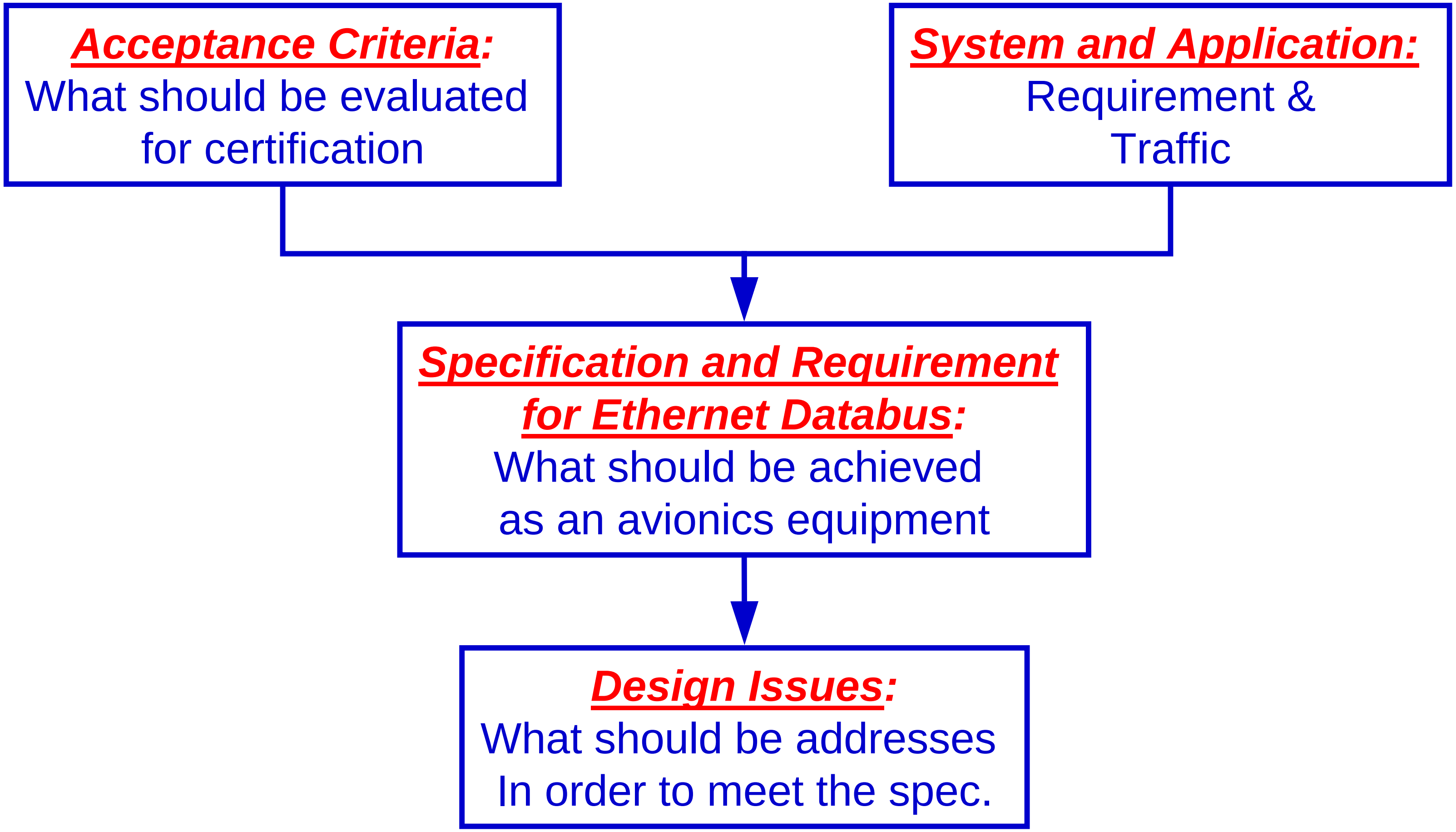
- **Step 3: Analysis and verification -- How the application-level requirements are met**
  - Packet scheduling in the switches
  - Packet and task scheduling in the end systems
  - End-to-end delay
  - Fault-tree analysis
  - Reliability analysis
  - Test scenarios and traffic patterns (average and worst cases)
  - Fault injection and recovery operation
  - Timing measurement

Handbook Development

Handbook Development

- **Integrate the research results in a handbook on *Certification and Design Considerations***
- **Idea of development**
  - CAST-16 paper as the base
  - Design and certification guidelines by providing elaborations on what should be addressed
    - less on how to do it
  - Acceptance criteria
    - general (DO-178B, etc.) and application specific (for databuses)
  - System specification and requirement
  - Design issues which have an impact on deterministic operations

Handbook Development (cont’d)



Acceptance Criteria:
What should be evaluated
for certification

System and Application:
Requirement &
Traffic

Specification and Requirement for Ethernet Databus:
What should be achieved
as an avionics equipment

Design Issues:
What should be addresses
In order to meet the spec.

Certification Considerations

- Goal: to demonstrate the achievement of safety, performance, and reliability
- CAST-16 paper: categories and criteria
  - General: applicable to all avionics products
  - Application specific: applicable to Ethernet databus
- Safety: determinism on data delivery (delays under failure-free and recovery modes)
- Data Integrity:
  - System level: node and link failures
  - Message level: message loss or bit-error-rate
- Performance: message bandwidth and latency
- System Configuration: communication entities, topology, traffic management, and message routing

Ethernet Databus Requirements

- **What Ethernet databus must do for the avionics systems?**
- **Determinism – guaranteed message delivery with a bounded latency**
  - at system level, node and switch levels
  - dependability
  - what else should be guaranteed?
- **Requirements**
  - Traffic specification – models and parameters
  - Resource availability – at each node and switch
  - Quality of service – per application and connection
  - Error/failure management and protection

Design Issues (1)

- **What the inherent design problems that must be resolved for a certifiable Ethernet databus?**
- **Issues with CSMA/CD protocol**
  - bus-based cyclic scheduling –
    - time-based and synchronized
    - one transmitter at a time
  - switch-based message scheduling –
    - full-duplex and one transmitter on each bus
    - message routing and scheduling must lead to deterministic behavior

Design Issues (2)

- **Flow control –**
  - open-loop control (preferred) vs. close-loop
  - flow specification – to describe traffic flows in the network
    - worst case and average
  - traffic regulation –
    - shaping and policing schemes and mechanisms
    - any effect of violation
    - buffer requirement and message dropping
  - admission control
    - can a connection be accepted or rejected

Design Issues (3)

- **Deterministic Message Transmission in Switched Ethernet**
  - message arrival and departure processes
  - switch architecture, scheduling disciplines, and message buffers
  - guaranteed end-to-end QOS and message ordering
- **Data Integrity and Reliability**
  - lossless, fault isolation, and redundancy
  - any detection and recovery at higher layers (e.g. application)

Design Issues (4)

- **Network Stack Processing**
  - connection-oriented – state information, bandwidth allocation, sequence and flow control
  - address resolution – static and deterministic
  - addressing scheme – unicast and multicast, MAC, and connection
- **Non-determinism in Ethernet Interface Components**
  - interrupt, DMA, FIFO buffer management, context switching, etc.
  - PCI-based components as an example
- **System Configuration**

Main Notions

- **Certification criteria about safety, performance, and data integrity**
- **System requirements → network requirements**
- **Application model → traffic model**
- **Demonstration**
  - feasible approaches -- such as static routing, fixed addressing, open-loop control, traffic model, connection-oriented, etc.
  - provable algorithms (deterministic and bounded worst-case behavior)
  - evaluation of implementation (software and hardware at component and system levels)

Summary and Conclusions

Summary and Conclusions

- **High speed databus for avionic system is in demand**
  - Use COTS technology for critical applications
  - Deterministic
- **Certification for aviation databus**
  - “Do the right thing” and “Make the thing right”
  - What are required by the applications
  - What are needed in architecture and component designs
  - What should be done to demonstrate the processes and the results
- **Difficult to come up check boxes, but need a structured approach to address**
  - Requirement
  - Design and implementation
  - Analysis, testing, and verification

Contact Information

ARIZONA STATE UNIVERSITY

www.asu.edu

Yang-Hang Lee (yhlee@asu.edu)

Honeywell

www.honeywell.com

Elliott Rachlin (elliott.rachlin@honeywell.com)

Phil Scandura (philip.scandura@honeywell.com)

FEDERAL AVIATION ADMINISTRATION

www.faa.gov

Charles Kilgore
(charles.kilgore@tc.faa.gov)

Software & Digital Systems Safety Research Program
FAA William J. Hughes Technical Center
Flight Safety Research Branch, AAR-470
Atlantic City, New Jersey

Handbook Outline

1. **Introduction: purpose, scope, organization, and focus for readers**
2. **Ethernet-based Aviation Databus System**

   2.1 A Brief Overview Of Ethernet

   2.2 General Concerns of Ethernet as an Avionics Databus

3. **Certification of Ethernet-based Avionics Databus**

   3.1 Background

   3.2 Certification Considerations

   3.3 Certification Position Paper

   3.4 Generic Evaluation Criteria

   3.5 Ethernet Databus Specific Evaluation Criteria

   3.6 Use of COTS Products

Handbook Outline (cont’d)

4. Avionics Application Requirements

4.1 Determinism in Communication system

4.2 Avionics Application Requirements

5. Issues To Be Addressed by Ethernet-based Databus Designers

5.1 Issues with CSMA/CD Protocol

5.2 Flow Control

5.3 Deterministic Message Transmission in Switched Network

5.4 Data Integrity and Reliability

5.5 Network Stack Processing

5.6 Non-determinism In Hardware Components On End System

5.7 System Configuration

6. Conclusion